COMPLETE LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings of claims in the application. Applicants have submitted a new complete claim set showing marked up claims with insertions indicated by underlining and deletions indicated by strikeouts and/or double bracketing.

Listing of Claims

1–33. (Canceled)

34. (Previously Presented) A dynamic email spam analysis and management system comprising:

a database including a plurality of spam rules, each of the plurality of spam rules having attributes including a score;

a spam analyzer operable to process a log file received from each of a plurality of message switches, each message switch processing an email against each of the plurality of spam rules thus determining if the processed email will be marked as spam, and for each match between the processed email and each of the plurality of spam rules, each message switch creating an entry in its log file corresponding to the processed email and the matching spam rule wherein each entry includes the score from each matching spam rule, the spam analyzer ~~and~~ operable to update the attributes of at least one of the plurality of spam rules in the database, the updating including modifying the score of the at least one of the plurality of spam rules, the updating based on statistics calculated from at least one of the log files, wherein the spam analyzer is distinct from each of the plurality of message switches, and wherein each of

the plurality of message switches are software being executed on one of a plurality of mail servers; and

a select rules file including one or more select rules from the database of the plurality of spam rules, each of the one or more select rules being included in the select rules file based on its attributes, the select rules file being replicated to each of the message switches.

35.   (Previously Presented) The system of claim 34 wherein the spam analyzer processes each log file to determine how many times each of the plurality of spam rules was hit and accordingly updates the attributes corresponding to the each of the plurality of spam rules.

36.   (Previously Presented) The system of claim 34 wherein the attributes corresponding to each of the plurality of spam rules are updated to indicate how many times each of the plurality of spam rules was false–positive–hit.

37.   (Previously Presented) The system of claim 34 wherein one or more other select rules of the plurality of spam rules are retired, each of the one or more other select rules being retired based on its attributes.

38.   (Previously Presented) The system of claim 37 wherein the one or more other select rules have not been hit within a predetermined amount of time.

39.   (Previously Presented) The system of claim 34 wherein the select rules file further includes one or more new rules.

40.   (Previously Presented) The system of claim 34 wherein the spam analyzer calculates, based on information derived from the log file, how many times each of the plurality of spam rules was hit.

41.   (Previously Presented) The system of claim 34 wherein the attributes of each of the plurality of spam rules are modified to indicate how many times each of the plurality of spam rules was false-positive-hit.

42.   (Previously Presented) The system of claim 34 wherein the spam analyzer calculates, based on information derived from the log file, how many hits of each of the plurality of spam rules was determined to be for spam email messages and accordingly modifies the corresponding attributes of the each of the plurality of spam rules.

43.   (Previously Presented) The system of claim 34 wherein the spam analyzer calculates based on information derived from the log file, how many hits of each of the plurality of spam rules was determined to be for non-spam email messages and accordingly modifies the corresponding attributes of the each of the plurality of spam rules.

44.   (Previously Presented) The system of claim 34 wherein the score of one of the plurality of spam rules is modified manually.

45.   (Currently Amended) A dynamic email spam analysis and management system comprising:

  a message switch including a spam filter operable to receive an email message wherein the message switch is one of a plurality of message switches that are each software being executed on one of a plurality of mail servers comprising a conventional server; and

  a select rules file including a plurality of spam rules, each of the plurality of spam rules having attributes including a score, wherein the spam filter analyzes the email message to determine if the email message will be marked as spam wherein the analyzing includes creating an entry in a log file, the entry including the score from each of the plurality of spam rules that matches the email message, and wherein the message switch periodically communicates the contents of the log file to a central server and periodically receives an updated select rules file from the central server, the updated select rules file differing from the select rules file, and the updated select rules file becoming the select rules file once received, and wherein the central server is distinct from each of the plurality of message switches.

46.   (Canceled)

47.   (Previously Presented) The system of claim 45 wherein a total spam score for the email message is modified using the score of each of the plurality of spam rules for which there is a hit on the email message.

48.   (Previously Presented) The system of claim 47 wherein, if the total spam score exceeds a score threshold, the email message is identified as a spam email message.

49.   (Previously Presented) The system of claim 45 wherein each of the plurality of spam rules has attributes including one or more of: a date and time the spam rule was last updated, number of hits, number of spam hits, number of non-spam hits, and date and time of last hit.

50.   (Previously Presented) The system of claim 47 wherein, if the total spam score does not exceed a score threshold, the email message is identified as a non-spam email message.

51.   (Previously Presented) The system of claim 50 wherein the email message is transferred to an intended recipient.

52.   (Previously Presented) The system of claim 45 wherein each of the plurality of spam rules are constructed using regular expressions.

53.   (Previously Presented) A method for dynamically updating spam rules, the method comprising:

receiving an email message at a message switch wherein the message switch is one of a plurality of message switches that are each software being executed on one of a plurality of mail servers;

processing the email message against the spam rules to determine if the email message will be marked as spam, each of the spam rules having attributes including a score;

creating a spam information entry in a log file, the spam information entry including the score from each of the spam rules that the processed email message matches;

calculating statistics for the spam rules based on the spam information in the log file;

updating a database of the spam rules based on the statistics, the updating including modifying the score of at least one of the spam rules;

selecting a set of select rules from the database of the updated spam rules to form a select rules set; and

replicating the select rules set to the message switch wherein the select rules set, once received by the message switch, becomes the spam rules.

54–55. (Canceled)

56.   (Previously Presented) The method of claim 55 wherein the processing includes testing the email message against each of the spam rules for a hit and, if a hit exists for the each of the spam rules, modifying a total spam score of the email message based on the score of the each of the spam rules.

57.   (Previously Presented) The method of claim 56 wherein the spam information entry corresponding to the email message in the log file includes an identifier for each of the spam rules for which there was a hit.

58.   (Previously Presented) The method of claim 53 wherein the calculating includes calculating, based on the log file, how many times each of the spam rules was hit.

59.   (Previously Presented) The method of claim 53 wherein the calculating includes calculating, based on the log file, how many hits for each of the spam rules were for a spam email message versus a non–spam email message.

60. (Previously Presented) The method of claim 53 wherein the updating includes updating a quantity of false-positive-hits for one or more of the spam rules.

61. (Previously Presented) The method of claim 53 wherein the selecting includes retiring one or more of the spam rules wherein the retired spam rules are not included in the select rules set.

62. (Previously Presented) The method of claim 55 wherein the updating includes updating the score of one or more of the spam rules based on the statistics.

63. (Previously Presented) The method of claim 55 wherein the score of each of the spam rules can be modified manually.

64. (Previously Presented) The method of claim 53 wherein the replicating includes replicating the select rules set to each of the plurality of message switches.

65. (Previously Presented) The method of claim 53 further comprising, if the email message is determined to be a non-spam email message, transferring the email message to an intended recipient.

66. (Previously Presented) The method of claim 53 embodied as computer-executable instructions stored on a computer-readable medium.